Method for Evaluating the Internal Physical Structure of Adversary Orbital Platforms to Facilitate Robotic Covert Access to and Modification of Internal Systems for Eavesdropping

8 November 2022
Simon Edwards
Research Acceleration Initiative

Introduction

For years, platforms such as X-37 have been used in a maintenance role for refueling and repairing friendly satellites. This process is made easy by having schematics of friendly systems at our disposal to guide any repair process.

Schematics of the internals of adversary orbital platforms are amongst the most closely guarded secrets of any nation and are therefore rarely available. To be able to decrypt communications sent through a hostile military communication network, particularly quantum key encrypted data, it is necessary to "bug" the adversarial orbital platform to collect data concerning encryption keys and perhaps even remove physical modules for later analysis in cases where the technology may be more advanced than our own. Systems aboard satellites have redundancies and thus the removal of a single module could be misattributed by an adversary to the failure of a component.

Abstract

To be able to know how to "find one's way around" inside of a foreign platform requires more than simply inserting a robotic arm with a flashlight attached into the adversary satellite to try to pick out what looks like a co-processor or a RAM module. To be able to plant bugs in a location of use and in a timely manner, detailed schematics must be available for study in advance so that robotic espionage may proceed.

Although space is a vacuum, gasses, counterintuitively, can be used to our advantage in the arena of space in support of the cause of building an internal map of an adversary orbital platform with an unknown internal configuration.

Such a map could be constructed by dispatching an X-37 platform complete with the customary robotic armature to an adversary's satellite with the addition of a few tools not traditionally carried by the platform. The X-37 would require a supply of radioactive hydrogen (3H/tritium,) a heater for heating the tritium to maintain its gaseous state, a LASER for creating a pinhole in an adversarial platform and a thin nozzle (or perhaps an airtight seal fitting over the exterior) for injecting the radioactive gas into the pinhole.

The tritium would diffuse into the various crevices of the platform and accumulate as a powder-like solid on the surface of components. In addition to its property of visible luminescence, tritium gives off energy in the far-infrared and T-Ray range capable of penetrating the walls of the platform and being detected from the outside using cameras designed to photograph emissions in these ranges. These photographs would detail both the contours of the components within the adversary platform but would also pinpoint the

primary pathways in circuits within the platform as tritium's radiative output is enhanced by electrical fields. Such information is critical for informing us as to where cuts must be made when a needed component cannot simply be accessed by removal of a panel. The espionage platform would also need to know where NOT to cut since many wires and components are concentrated in a confined area. Accidental damage to the platform would defeat the purpose of bugging the platform and may alert an adversary to tampering.

Conclusion

Thanks to the remarkable sensitivity of the far-IR and T-Ray sensors involved, it is possible to ascertain in this manner the ideal position in which to place a bug within an adversary platform given this reconnoitering step and time to analyze the data. Just as it has been common practice for nearly 30 years to extract encryption keys from RAM to side-step the strength of modern encryption (i.e. the essence of a Tailored Access Operation,) the very same principle dictates the use of a similiar approach to overcome modern military SATCOM encryption including upcoming quantum-entanglement based communication, current-generation Evolving One-Time-Pad (EOTP) systems and other cryptanalysis-resistant methods likely to be employed by any highly competent adversary.